PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Examiner: Mohammad W. Reza
Ibrahim, et al.	
	Art Unit: 2436
Serial No.: 10/827,218	
Filed: 4/19/04	Confirmation No.: 2929
For: SUBORDINATE TRUSTED PLATFORM MODULE	
Date of Final Office Action: January 29, 2009	Attorney Docket No.: 200314912-1
Notice of Appeal Filed: April 13, 2009	

June 11, 2009

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

This Appeal Brief is timely provided to support the Notice of Appeal filed April 13, 2009.

1. Real Party in Interest:

The real party in interest is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 11445 Compaq Center Drive West, Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

2. Related Appeals and Interferences

There are no other prior and/or pending appeals, interferences, or judicial proceedings that are related to, directly affect, or that will be directly affected by or have a bearing on the Board's decision.

3. Status of Claims

Claims 1-18, 45-46 and 48-49 are pending in the application.

Claims 1-18, 45-46 and 48-49 stand rejected.

Claims 19-44 and 47 were canceled.

No claims were allowed.

The rejections of claims 1-18, 45-46 and 48-49 are appealed.

4. Status of Amendments

No Amendments were filed subsequent to the Final Office Action.

5. Summary of Claimed Subject Matter

Independent Claim 1

Independent claim 1 recites a system that comprises a logic configured to perform cryptographic key maintenance for a trusted platform to which the logic is bound in a one-to-one manner (specification, page 7, lines 7-11; Figure 1, logic 110). The cryptographic key maintenance includes migrating a non-migratable storage root key from a root of a key storage hierarchy associated with a trusted platform module associated with the trusted platform (specification, page 8, lines 1-4). Additionally, the system comprises an interface configured to facilitate operably connecting the system to the trusted platform (specification, page 7, lines 11-13; Figure 1, interface 130).

Independent Claim 5

Independent claim 5 recites a logic configured to perform one or more of, cryptographic key maintenance, and cryptographic key migration for a trusted platform to which the logic is bound in a one-to-one manner (specification, page 7, lines 7-11; Figure 1, logic 110). The system also comprises an interface configured to facilitate operably connecting the system to the trusted platform (specification, page 7, lines 11-13; Figure 1, interface 130). The logic and the interface comprise part of a USB token (specification, page 7, lines 16-18).

Dependent Claim 6

Dependent claim 6 recites where the logic is configured to migrate one or more non-migratable keys from a trusted platform module associated with the trusted platform (specification, page 8, lines 1-4). In addition, the logic is configured to use the migrated one or more non-migratable keys to decrypt items that were encrypted by the trusted platform module (specification, page 9, lines 2-4).

Dependent Claim 7

Dependent claim 7 recites where the logic is configured to perform cryptographic key maintenance including cloning the trusted platform with the cooperation of a manufacturer of the trusted platform and an owner of the trusted platform (specification, page 7, line 31 to page 8, line 1).

Dependent Claim 17

Dependent claim 17 recites where binding the logic to the trusted platform in a one-to-one manner includes producing an optimal asymmetric encryption padding (OEAP) binary large object (specification, page 9, lines 17-20). This is done to facilitate copying a storage root key stored in a trusted platform module associated with the trusted platform (specification, page 13, lines 21-24).

Independent Claim 45

Independent claim 45 recites an electronic apparatus configured with a trusted platform module and an interface operably connected to the electronic apparatus (specification, page 19, lines 6-9; Figure 6, computer 600). The interface is configured to facilitate operably, detachably connecting a subordinate trusted platform module to the electronic apparatus (specification, page 19, lines 6-9). The system further comprises a subordinate trusted platform module to communicate with the trusted platform module via the interface (specification, page 17, lines 25-27). The subordinate trusted platform module including logic to migrate a non-migratable storage root key from the trusted platform module to be stored within the subordinate trusted platform module (specification, page 7, line 30 to page 8, line 4 and specification, page 7, lines 8-9).

6. Grounds of Rejection to be Reviewed on Appeal

I. Whether claims 1-18, 45-46, and 48-49 are unpatentable under 35 U.S.C. §112, first paragraph, as failing to comply with the enablement requirement.

II. Whether claims 1-18, 45-46, and 48-49 are unpatentable under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

III. Whether claims 1-18, 45-46, and 48-49 are unpatentable under 35 U.S.C. 103(a) as being obvious over Challener et al. (U.S. Publ. 2003/0105965), in view of Cromer et al. (US Patent 7,191,464).

7. Argument

I. Whether claims 1-18, 45-46, and 48-49 are unpatentable under 35 U.S.C. §112, first paragraph, as failing to comply with the enablement requirement.

35 U.S.C. §112, first paragraph recites:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1-18, 45-46, and 48-49 comply with the enablement requirement set in the statute. The issue is that the Examiner could not find in the specification an explanation of how to migrate a non-migratable storage root key (Final Office Action (FOA), page 3, lines 1-4). However, the specification clearly contains a written description to enable any person skilled in the art to migrate a non-migratable storage root key. For example, page 8, lines 1-8 of the specification explains how migrating a non-migratable storage root key can be implemented in one embodiment. For The Board's convenience, page 8, lines 1-8 of the specification is repeated here:

> Additionally, and/or alternatively, cryptographic key maintenance may include having the manufacturer of the trusted platform 120 act as an intermediary and migrating a non-migratable storage root key from a root of a key storage hierarchy associated with a trusted platform module associated with the trusted platform 120. Cryptographic key migration may include, for example, logically attaching a TPM migratable key data structure from one protected storage tree to another protected storage tree. In one example, the cryptographic key maintenance and the cryptographic key migration performed by the logic 110 comply with the Trusted Computing Group (TCG) specification version 1.1b. [emphasis added]

Clearly, the above text from the specification enables one skilled in the art to migrate a non-migratable storage root key. The text provides an example for a migration operation, an entity that can perform the operation (logic 110), and a standard for use in performing the operation (TCG specification version 1.1b). While the example does not limit the claims, the example clearly shows that the enablement requirement is met by the written description. There is no requirement that every possible way to perform the migration be disclosed. Since an adequate written description for the term in question as required by statute is presented, the rejection should be reversed.

II. Whether claims 1-18, 45-46, and 48-49 are unpatentable under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention.

35 U.S.C. §112, second paragraph recites:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-18, 45-46, and 48-49 are definite as required by 35 U.S.C. §112, second paragraph. The Examiner finds the following feature from claim 1 indefinite: a key storage hierarchy associated with a trusted platform module associated with the trusted platform. (FOA, page 3-4, section 8, lines 3-6). The Examiner states "[e]xaminer failed to understand what is difference between these two trusted platforms from the claim." (FOA, page 3, section 8, lines 9-11). It is unclear from where the Examiner is reading two trusted platforms in claim 1.

Claim 1 recites "...a key storage hierarchy associated with a trusted platform module associated with the trusted platform..." Thus, claim 1 recites a trusted platform and a trusted platform module. Claim 1 does not recite two trusted platforms as the Examiner asserts. The specification states "[a] 'trusted platform', is a platform that includes a trusted platform module, as that term is defined by the TCG" (specification, page 5, line 18-19). In addition, Figure 1 shows a trusted platform module (a subordinate trusted platform module 100) and a trusted platform 120 associated with one another. As can be seen, the specification clearly shows how there can be a trusted platform module associated with the trusted platform as claim 1 recites. Therefore, the examiner's reading of the claim is incorrect. The statutory requirement is met for claim 1 and the rejection should be reversed.

Regarding independent claim 45, the phrase in question, "a trusted platform module associated with the trusted platform" is not recited. Therefore, the rejection of claim 45 is a clear error and should be reversed.

III. Whether claims 1-18, 45-46, and 48-49 are unpatentable under 35 U.S.C. 103(a) as being obvious over Challener et al., in view of Cromer et al. (US Patent 7,191,464)

Appellant notes that the FOA refers to "Weiss (US patent 6071190)" as the citation to Challener (FOA, page 4, section 9). Appellant confirmed with the examiner by telephone that the reference to Weiss was in error. The correct citation is Challener et al. – U.S. Publ. 2003/0105965 (hereinafter "Challener").

To establish a prima facie case of 35 U.S.C. §103 obviousness, basic criteria must be met. The prior art reference (or references when combined) must teach or suggest all the claim limitations. MPEP 2143(A). Section 2131 of the MPEP recites how "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2

USPQ2d 1051, 1053 (Fed. Cir. 1987). This same standard applies to 103 rejections as evidenced by Section 2143(A) of the MPEP, which reads: "The rationale to support a conclusion that the claim would have been obvious is that **all the claimed elements** were known in the prior art and one skilled in the art could have combined the elements as claimed by known methods with no change in their respective functions".

Independent Claim 1

A. Claimed Element: migrating a non-migratable storage root key

Claim 1 recites a system comprising "logic configured to perform cryptographic key maintenance ... where the cryptographic key maintenance includes migrating a non-migratable storage root key from a root of a key storage hierarchy..." Challener and Cromer, neither individually nor combined, teach or suggest this claim feature.

The Examiner states that Challener teaches or suggests this claim feature (FOA, page 4, section 10, lines 1-7). Specifically, Challener's abstract and paragraphs 0003-0031 are cited against claim 1 (FOA, page 4, section 10, lines 1-7). The examiner's interpretation is incorrect. Challener explicitly discloses that non-migratable keys cannot be and are not migrated:

> "Non-migratable" keys are locked to the hardware in a way that they cannot be cloned or migrated to another system even by the owner." (Challener, paragraph 26, lines 12-14) [emphasis added]

Thus, Challener clearly discloses that non-migratable keys cannot be migrated. Challener provides no teaching or suggestion of anyway to the contrary. Challener fails to consider such a migration. As such, Challener fails to provide any teaching or suggestion to one of ordinary skill in the art reading the disclosure that a non-migratable storage root key is migratable.

Challener's teaching is opposite of what is claimed. Claim 1 recites logic that migrates a non-migratable storage root key. Therefore, Challener fails to teach or suggest the claimed elements and fails to support the rejection. A prima facie obviousness rejection has not been established and the rejection should be reversed.

In addition to not teaching or suggesting migrating non-migratable keys in general, Challener does not disclose migrating a non-migratable "storage root key" as claimed. The only mention of a storage root key in Challener is from paragraph [0027], line 26 to paragraph [0028], line 9. The following sentence-by-sentence analysis of the cited text yields no teaching or suggestion of what is claimed.

Challener [0027], line 26 to [0028], line 9: Sentence-by-sentence	Teaches migrating a non-migratable storage root key?
The customer also decides what parent will be used for storing this key (the SRK (storage root key) is available).	No.
The key stored is called a child, while the key used to do the storing is called the parent.	No.
In particular, if there are two key pairs, Private One, Public One and Private Two, Public Two, if Private Two is encrypted with Public One, then the first key pair would be referred to as the parent and the second key pair the child.	No.
Further, there is one key that is guaranteed to always be loaded inside the chip.	No.
It is called the storage root key, and it is an ancestor of	No.

every other key the chip can use.	
To load a key into the chip, it needs to have its parent's private key already loaded in the chip (so the chip can decrypt it).	No.
If the SRK is the great grandparent of a key, first one would need to load the grandparent of a key in the chip, then the parent of the key into the chip, and finally the key itself into the chip.	No.
This structure, called a daisy chain, is used to allow a TCPM chip to "store" an unlimited number of keys.	No.
The customer will then execute a TPM_CreateWrapKey command, with required parameters indicating the key produced will be a storage key.	No.
The customer then signs the non-migratable storage key, K1, with the TPM identity key, P2, creating a certificate, C3, for that non-migratable storage key.	No.
In another alternative embodiment of step 202, the customer creates a non-migratable signing key, K2, with the TPM_CreateWrapKey command, wherein the key may be a 2048-bit RSA key.	No.
Signing keys can be used by the TPM to sign the hash of a message (i.e., encrypt the hash of a message).	No.
The customer decides if this signing key, K2, will require authorization or not, and what that authorization will be.	No.

The customer decides what parent will be used for storing this key (the SRK is available).	No.

The above analysis shows that the claim feature is not taught or suggested in Challener. Therefore, Challener does not teach or suggest logic configured to migrate a non-migratable storage root key as claimed. The claimed element is not found and the rejection is not supported. The interpretation of Challener is in clear error and the rejection should be reversed.

B. Claimed Element: logic is bound in a one-to-one manner

Claim 1 also recites "...a trusted platform to which the logic is bound in a one-to-one manner..." Challener and Cromer do not teach or suggest this claim feature.

The Examiner admits that Challener does not disclose this claim feature (FOA, page 4, section 10, last line to page 5, line 1). Appellant agrees. The Examiner cites Cromer as teaching or suggesting this feature (FOA, page 5, lines 1-7). Specifically, the Examiner cites col. 4, lines 35-55 and col. 4, lines 50-62 of Cromer against the claim feature (FOA, pages 4-5, section 10, lines 8-10). The interpretation and reliance on Cromer is incorrect.

Cromer discusses shadow registers linked one-to-one to boot registers, and not the claimed logic bound one-to-one with a trusted platform. In particular, Cromer states, "...an embedded security system...includes at least one boot platform configuration register (PCR) and a shadow PCR for the boot PCRs..." (col. 3, lines 55-58). Cromer then states "[a]s is shown, the TPM (Trusted Platform Module) 44' includes a plurality of shadow PCRs 48a' that are linked, one-to-one, to the plurality of boot PCRs 48a." (col. 4, lines 36-38).

Merely reciting the term ‘one-to-one’ is not sufficient to teach or suggest the specifically claimed configuration. Cromer teaches a different configuration: shadow registers linked one-to-one to boot registers. Thus Cromer fails to teach or suggest the claimed logic bound one-to-one with a trusted platform. The claimed element is not found.

Cromer fails to support the rejection for which it is relied upon. Therefore, the combination of Challener and Cromer fail to teach or suggest each and every claimed element. A prima facie obviousness rejection has not been established and the rejection should be reversed.

Independent Claim 5

Claim 5 recites “...where the logic and the interface comprise part of a USB token.” Challener and Cromer do not teach or suggest this claim feature.

The Examiner states that Challener teaches or suggests this claim feature (FOA, page 5, section 14, lines 1-5). Specifically, Challener’s abstract and paragraphs 0003-0031 are cited against the claim (FOA, page 5, section 14, lines 1-5). A USB token is not discussed in Challener or Cromer. Specifically, Challener and Cromer are silent regarding a logic and interface that comprise part of a USB token. Therefore, the claim feature is not taught or suggested by Challener and Cromer. The rejection is not supported and should be reversed.

Claim 5 also recites “...a trusted platform to which the logic is bound in a one-to-one manner...” Similar to the reasons discussed in claim 1, the feature is not taught or suggested by Challener and Cromer. Therefore, the rejection should be reversed.

Dependent Claim 6

Claim 6 recites "...the logic is configured to migrate one or more non-migratable keys..." Similar to the reasons discussed in claim 1, the feature is not taught or suggested by Challener and Cromer. Therefore, the rejection should be reversed.

Dependent Claim 7

Claim 7 recites "[t]he system of claim 1, where the logic is configured to perform cryptographic key maintenance including cloning the trusted platform with the cooperation of a manufacturer of the trusted platform and an owner of the trusted platform." Challener and Cromer do not teach or suggest this claim.

The Examiner states that Challener teaches or suggests this claim (FOA, page 6, section 16, lines 1-4). Specifically, Challener's paragraphs 0022-0024 are cited against claim 7 (FOA, page 6, section 16, lines 1-4). A sentence-by-sentence analysis of the cited text yields no teaching or suggestion of what is claimed:

Challener: paragraphs [0022] to [0024]: Sentence-by-sentence	Teaches logic configured to perform cryptographic key maintenance including cloning the trusted platform?
Referring to FIGURE 2, there is illustrated a flow diagram of a process configured in accordance with an embodiment of the present invention where a potential credit card customer desires to receive an embedded	No.

credit card authorization within the customer's computer system 301.	
In step 201, the customer will create a TPM identity per the TCPA Specification and obtain a certificate for it. The TCPA Specification is published at www.trustedpc.org/home/home.htm,as Version 1.1b, which is hereby incorporated by reference herein.	No.
When a TPM is manufactured, its own endorsement key is generated and placed into nonvolatile memory inside the TPM chip.	No.
Only the public portion of that endorsement key, P1, is ever released from the chip, and is released to the manufacturer.	No.
The manufacturer of the TPM signs a certificate, C1, that goes along with the TPM.	No.
Alternatively, the certificate, C1, can be retrieved by a user over the Internet from the manufacturer.	No.
This certificate, C1, is tied to the public portion of the endorsement key, P1, that determines that the public key is the endorsement key of this particular TPM. This endorsement key, P1, is used for decrypting.	No.
As noted above, a TPM identity is created in step 201, which is a special kind of private key.	No.
A TPM identity can be created by the customer, such as with a DOS command, and the TPM identity is the public	No.

portion of a public/private key pair.	
The public key, P2, of the TPM identity and the certificate, C1, tied to the public portion of the endorsement key, P1, are then sent over the Internet to a Certificate Authority (CA).	No.
This may be authorized by the user as a result of a user command. The CA checks the accuracy of the certificate, C1, signed by the manufacturer.	No.
The CA can perform this check by looking in a database at the manufacturer's website.	No.
The CA then makes a certificate, C2, for the TPM identity, P2, and encrypts the certificate, C2, and bundles it with the public key, P2, of the TPM identity sent by the customer.	No.
This second bundle is then encrypted with the public endorsement key, P1, of the TPM.	No.

It is clear that the above text from Challener does not relate to logic configured to perform cryptographic key maintenance including cloning the trusted platform with the cooperation of a manufacturer of the trusted platform and an owner of the trusted platform as claimed. Therefore, Challener and Cromer do not teach or suggest claim 7.

In addition, Challener only once mentions cloning and Cromer is silent regarding cloning. Challener states “’[n]on-migratable’ keys are locked to the hardware in a way that they cannot be cloned or migrated to another system even by the owner." [emphasis added] Challener never teaches or suggests cloning a trusted platform as claimed. Therefore, the claim feature is not taught or suggested by Challener or Cromer and the rejection should be reversed.

Dependent Claim 17

Claim 17 recites "[t]he system of claim 1, where binding the logic to the trusted platform in a one-to-one manner includes producing an optimal asymmetric encryption padding (OEAP) binary large object to facilitate copying a storage root key stored in a trusted platform module associated with the trusted platform." Challener and Cromer do not teach or suggest this claim feature.

The Examiner states that Challener teaches or suggests the claim feature (FOA, page 8, section 26, lines 1-5). Specifically, Challener's paragraph 0020 is cited against the claim (FOA, page 8, section 26, lines 1-5).

The Examiner's statement conflicts with his previous position under claim 1. There, the Examiner stated "[h]e (Challener) does not expressly disclose the logic is bound to in a one-to-one manner with trusted platform" (FOA, pages 4-5, section 10, lines 7-8). It is confusing to Appellant how Challener does not teach or suggest logic bound in a one-to-one manner yet purportedly teaches or suggests what is included in binding the logic to the trusted platform in a one-to-one manner. Challener does not show binding the logic to the trusted platform in a one-to-one manner as well as what the binding includes as claimed.

Regardless of the conflicting statements, a sentence-by-sentence analysis of the relied-upon section of Challener paragraph [0020] yields no teaching or suggestion of what is claimed:

Challener: paragraph [0020]: Sentence-by-sentence	Teaches claimed binding?
Implementations of the invention include implementations as a computer system programmed to execute the method or methods described herein, and as a computer program product.	No.
According to the computer system implementation, sets of instructions for executing the method or methods may be resident in the random access memory 114 of one or more computer systems configured generally as described above.	No.
Until required by the computer system, the set of instructions may be stored as a computer program product in another computer memory, for example, in disk drive 120 (which may include a removable memory such as an optical disk or floppy disk for eventual use in the disk drive 120).	No.
Further, the computer program product can also be stored at another computer and transmitted when desired to the user's workstation by a network or by an external network such as the Internet 303.	No.
One skilled in the art would appreciate that the physical storage of the sets of instructions physically changes the medium upon which it is stored so that the medium carries computer readable information.	No.

The change may be electrical, magnetic, chemical, biological, or some other physical change.	No.
While it is convenient to describe the invention in terms of instructions, symbols, characters, or the like, the reader should remember that all of these and similar terms should be associated with the appropriate physical elements.	No.

It is clear that the above text does not relate to binding the logic to the trusted platform in a one-to-one manner that includes what is claimed. Additionally, Cromer is silent regarding what is claimed. Therefore, this claim feature is not taught or suggested by Challener and Cromer and the rejection should be reversed.

Independent Claim 45

Claim 45 recites "...the interface configured to facilitate operably, detachably connecting a subordinate trusted platform module to the electronic apparatus..." Challener and Cromer do not teach or suggest this claim feature or the claim as a whole.

The Examiner admits that Challener does not disclose this feature (FOA, pages 8-9, section 28, lines 7-9). Appellant agrees. The Examiner cites Cromer as teaching or suggesting the feature (FOA, page 9, section 28, lines 9-12). Specifically, the Examiner cites col. 4, lines 35-55 and col. 3, lines 50-62 as disclosing the claim feature (FOA, page 9, section 28, lines 10-13). The examiner's reliance is incorrect.

Cromer column 4, lines 35-55 reads:

> FIG. 3 illustrates a TPM in accordance with the method and system of the present invention. As is shown, the TPM 44' includes a plurality of shadow PCRs 48a' that are linked, one-to-one, to the plurality of boot PCRs 48a. During the boot sequence, measurements from each component are extended to the boot PCRs 48a and to the corresponding shadow PCRs 48a'. Each shadow PCR 48a' corresponds directly to each boot PCR 48a. Upon a platform reset, the boot PCRs 48a reset to zero, but the shadow PCRs 48a' retain their respective values. Thus, if an intruder boots rogue software and/or data from a removable medium, and performs a platform reset, the boot PCR 48a values reset to zero, but the shadow PCRs 48a' do not. The ensuing boot sequence, which again measures each bootable device and extends those values to the boot PCRs 48 and shadow PCRs 48a', will result in boot PCR 48a values that differ from the shadow PCR 48a' values. This indicates that unauthorized software or another operating system was booted since the last time the trusted operating system 14 was booted and prompts the trusted operating system 14 to take measures to restore trust.

The cited text relates to what is included in a TPM (Trusted Platform Module). Additionally, the cited text discusses what occurs during a boot sequence and a platform reset. No disclosure is found related to detachably connecting a subordinate trusted platform module to an electronic apparatus as claimed. Therefore, the cited text does not teach or suggest the claim feature.

Cromer column 3, lines 50-62 reads:

> [t]he present invention provides a method, system and computer readable medium containing programming instructions for tracking a secure boot in a trusted computer system having a plurality of devices. The method, system and computer readable medium include providing an embedded security system (ESS) in the computer system, wherein the ESS includes at least one boot platform configuration register (PCR) and a shadow PCR for the boot PCRs, initiating a platform reset to boot the computer system via BIOS, and, for each device booted, generating a measurement value for the device and extending that value to one of the at least one boot PCRs and its corresponding shadow PCR.

This text relates to providing an embedded security system. No disclosure is found relating to operably, detachably connecting a subordinate trusted platform module to an electronic apparatus as claimed. Therefore, the claim feature is not taught or suggested by Cromer. Cromer fails to cure the deficiencies of Challener and fails to establish a prima facie obviousness rejection. Each and every claimed element is not found in the combined references and the rejection should be reversed.

Claim 45 also recites "...migrate a non-migratable storage root key..." For reasons similar to those discussed in claim 1, Challener and Cromer do not teach or suggest this claim feature. Therefore, the rejection should be reversed.

Conclusion

For the reasons set forth above, a prima facie anticipation or obviousness rejection has not been established for any claim. All rejections have been shown to be improper. Appellant respectfully believes that all pending claims 1-18, 45-46 and 48-49 patentably and unobviously distinguish over the references of record and that the rejections should be reversed. Appellant respectfully requests that the Board of Appeals overturn the Examiner's rejections and allow all pending claims. An early allowance of all claims is earnestly solicited.

Respectfully submitted,

Peter Kraguljac (Reg. No. 38,520)

(216) 503-5500
Kraguljac & Kalnay, LLC
Summit One, Suite 510
4700 Rockside Road.
Independence, OH 44131

8. Claims Appendix

1. A system, comprising:

a logic configured to perform cryptographic key maintenance for a trusted platform to which the logic is bound in a one-to-one manner, where the cryptographic key maintenance includes migrating a non-migratable storage root key from a root of a key storage hierarchy associated with a trusted platform module associated with the trusted platform; and

an interface configured to facilitate operably connecting the system to the trusted platform.

2. The system of claim 1, where the cryptographic key maintenance performed by the logic comply with the Trusted Computing Group (TCG) specification version 1.1b.

3. The system of claim 1, where the logic comprises an application specific integrated circuit (ASIC).

4. The system of claim 1, where the logic comprises a microprocessor operably connected to a non-volatile memory.

5. A system comprising:

a logic configured to perform one or more of, cryptographic key maintenance, and cryptographic key migration for a trusted platform to which the logic is bound in a one-to-one manner; and

an interface configured to facilitate operably connecting the system to the trusted platform;

where the logic and the interface comprise part of a USB token.

6. The system of claim 5, where the logic is configured to migrate one or more non-migratable keys from a trusted platform module associated with the trusted platform and configured to use the migrated one or more non-migratable keys to decrypt items that were encrypted by the trusted platform module.

7. The system of claim 1, where the logic is configured to perform cryptographic key maintenance including cloning the trusted platform with the cooperation of a manufacturer of the trusted platform and an owner of the trusted platform.

8. The system of claim 7, where the logic is configured to perform cryptographic key maintenance including having the manufacturer of the trusted platform act as an intermediary and migrating the non-migratable storage root key from the root of the key storage hierarchy associated with the trusted platform module associated with the trusted platform.

9. The system of claim 1, where the logic is configured to perform cryptographic key migration including logically attaching a trusted platform module migratable key data structure associated with a first protected storage tree to a second protected storage tree.

10. The system of claim 1, where the logic is configured to store one or more of, a copy of a storage root key, a binding data that facilitates binding the logic to the trusted platform in a one-to-one binding, a processor executable set of instructions that facilitate the trusted platform determining that the trusted platform is interfacing with the logic instead of the trusted platform module, and a processor readable set of data that facilitates the trusted platform determining that the trusted platform is interfacing with the logic instead of a trusted platform module.

11. The system of claim 1, where the logic is configured to facilitate substantially instantaneously restoring the trusted platform module.

12. The system of claim 1, where the logic is configured to decrypt one or more of, a key, and a piece of data encrypted by the trusted platform module.

13. The system of claim 1, where the logic is configured to execute processor executable instructions associated with the logic while preventing execution of processor executable instructions not associated with the logic.

14. The system of claim 1, where the logic is configured to read processor readable data associated with the logic while preventing a second logic from reading the processor readable data associated with the logic.

15. The system of claim 1, where the logic is configured to detect whether there is a functional trusted platform module associated with the trusted platform.

16. The system of claim 1, where the logic is configured to prevent creation of a new cryptographic key by the system and to prevent performance of an attestation service by the logic.

17. The system of claim 1, where binding the logic to the trusted platform in a one-to-one manner includes producing an optimal asymmetric encryption padding (OEAP) binary large object to facilitate copying a storage root key stored in a trusted platform module associated with the trusted platform.

18. The system of claim 1, where the logic is configured to perform a finite number of cryptographic key maintenance operations.

19. – 44. (Canceled)

45. A system, comprising:

an electronic apparatus configured with a trusted platform module; and

an interface operably connected to the electronic apparatus, the interface configured to facilitate operably, detachably connecting a subordinate trusted platform module to the electronic apparatus; and

a subordinate trusted platform module to communicate with the trusted platform module via the interface, the subordinate trusted platform module including logic to migrate a non-migratable storage root key from the trusted platform module to be stored within the subordinate trusted platform module.

46. The system of claim 45, where the electronic apparatus comprises one of, a computer, a printer, a cellular telephone, and a digital camera.

47. (Canceled)

48. The system of claim 45 where the interface includes a port, and the subordinate trusted platform module is embodied in a removable component that is attachable and detachable to the port.

49. The system of claim 45 where the subordinate trusted platform module is configured to use the migrated non-migratable storage root key to decrypt items that were encrypted by the trusted platform module.

9. Evidence Appendix

None. There is no extrinsic evidence.

10. Related Proceedings Appendix

None. There are no related proceedings.